UNCLASSIFIED

BRIEFING NOTE FOR THE DEPUTY MINISTER AND CHIEF OF DEFENCE STAFF: ARTIFICIAL INTELLIGENCE AND COVID/L'INTELLIGENCE ARTIFICIELLE ET COVID

ISSUE

- Artificial Intelligence (AI), has played a critical role in containing and mitigating the impact of the ongoing COVID-19 pandemic.

- AI-enabled technology has brought many benefits to managing the pandemic, including accelerating medical research; detecting, diagnosing, and managing the virus' potential spread; enhancing supply chain security in important areas such as personal protective equipment and ventilators; and, developing useful apps (e.g. contact tracing apps for use by the public). Many countries are using these technologies in response to the virus, including Canada.

- Contact tracing applications (apps) in particular are increasingly being used in response to the COVID-19 pandemic. Concerns regarding location tracking, personal health data, and privacy in relation to these apps demonstrate how the use of AI enabled technologies can have potential negative impacts.

- At the same time, the use of these technologies raises many concerns from both defence and security, as well as public health perspectives. These concerns include: safely collecting and using data; bias in the use of these technologies; deploying these technologies too quickly; and the risk of irresponsible use.

- As the use of these technologies increases in the response to COVID, DND/CAF must consider their security implications and how to mitigate potential risks.

BACKGROUND

Key Uses of AI

- Artificial Intelligence (AI) has proven particularly useful in the response to COVID-19, including: understanding the virus and accelerating medical research on drugs and treatments; detecting and diagnosing the virus, and predicting its evolution; assisting in slowing the virus' spread through surveillance and contact tracing; and responding to the health crisis through personalised information and literacy campaigns.

Specific Use Cases

- In Canada, a research team at Lawson Health Research Institute in London, ON is working to determine whether trained AI can be used to diagnose COVID-19 by comparing lung ultrasound scans of infected patients to those without the disease.

UNCLASSIFIED

- Similarly, BlueDot, a Canadian start-up that uses AI to detect disease outbreaks, was one of the first to raise the alarm about a worrisome outbreak of a respiratory illness in Wuhan, China. Using machine learning algorithms, BlueDot sifts through news reports in 65 languages, as well as airline data and animal disease networks, to detect outbreaks and anticipate the dispersion of disease.

- Amazon recently implemented a "Distance Assistant," which uses camera footage in Amazon's buildings to identify high-traffic areas and remind individuals to maintain physical distance. Amazon is also testing a wearable device that lights up and delivers an audio alert when workers are too close to each other. While this technology is not yet widely implemented, it is likely that other firms similar in size and operations to Amazon will implement similar systems.

- AI is also being used to improve the reliability of supply chains across all sectors. The Joint Artificial Intelligence Center (JAIC) in the US is prototyping AI that can track data on ventilators, PPE, medical supplies and food to ensure health care professionals have access to the equipment they need and determine any logistics or supply chain issues or shortages. Further, JAIC has built a prototype AI tool that uses a wide variety of data streams to predict COVID-19 hotspots.

- Similarly, a team at DND/DRDC has built a prototype AI tool to help with the response to the pandemic as part of OP Laser. Specifically, DRDC scientists have developed a dynamic COVID-19 hot spot map showing the number of new COVID-19 cases reported weekly since January in Canada. The map is populated with publicly available data and the map will remain updated on a weekly basis to keep informing CAF planners and decision makers on the spread and prevalence of the virus.

Contact Tracing Apps

- Global momentum is building for the use of digital contact tracing to respond to the COVID-19 pandemic. This has generated many discussions among health practitioners, policy experts and companies alike on the appropriate use of this technology. While these apps may help public health authorities track and interrupt the transmission of COVID-19, their effectiveness and long term impacts remain uncertain.

- Contact tracing is the process of identifying, educating and monitoring individuals who have close contact with someone who has tested positive for the virus. Therefore, contact-tracing apps work by detecting and logging the presence of nearby devices.

- These apps can be broken down into four categories based on their goals: exposure notification (the goal of Canada's federal app); automated contact tracing (who has been near whom); symptom monitoring (for analysis and data collection); and epidemiological analysis (to identify hot spots or make public health predictions).

- Many countries are developing these apps in response to the crisis. The Government of Canada (GoC), for example, recently launched a national contact-tracing app. The GoC's app is intended to be completely anonymous. Using Bluetooth technology developed by

2/4

A0450342_2-000002

UNCLASSIFIED

Apple and Google, the app alerts users when they come into close contact with a diagnosed coronavirus patient.

- There are several major concerns over the use of these apps including: privacy, transparency and effectiveness. From a security perspective, this technology requires citizens' personal data. Malicious actors could potentially gain access to this data and use it for nefarious purposes.

CONSIDERATIONS

- While many have looked to AI as a saving grace during the pandemic, others have pointed to the technology's limitations highlighting that there are tremendous risks requiring careful consideration.

- The first consideration is data. AI requires massive amounts of data. As our health care system cannot release the information required to train AI systems (due to privacy and other information sharing regulations), no training data is available for the systems. This may lead companies to train their systems on data from other countries or regions, making it less relevant to Canadians.

- Further, COVID-19 tracking data poses great surveillance risks. Data storage may be decentralized (i.e., stored securely on individual devices) or centralized on servers maintained by governments or private companies. This increased data collection could allow potential malicious actors to use this data in ways that may endanger the public health system. For example, scammers could ask for additional information from individuals enrolled in contact-tracing apps. This runs the risk of any AI tool being co-opted for other purposes. It will be important to abide by data collection laws before implementing any technological surveillance.

- Second, consideration should be given to the consequences of quickly deploying these systems. When possible, before deploying future tools, efforts should be made to understand how they work and the potential for unintended consequences. Some health groups hurried to repurpose existing AI models to help track patients and manage the supply of beds, ventilators and other equipment in their hospitals. Similarly, researchers have tried to quickly develop AI models from scratch to focus on the unique effects of COVID-19, but many of these new tools have struggled with bias and accuracy issues. This means that that health care decisions informed by these systems could accelerate societal biases, potentially exacerbating negative health outcomes for vulnerable populations. Moving forward, consideration for how AI systems may accelerate societal biases must be part of each stage in the design and deployment of these technologies.

- Novel technologies (i.e. contact-tracing apps) that are untested are being increasingly used in the COVID-19 response. Therefore, the deployment of these technologies should be accompanied by clear communications regarding their limitations.

3/4

A0450342_3-000003

UNCLASSIFIED

- Finally, the privacy requirements of any technology used in the pandemic is a major consideration. In the deployment of any AI system designed to help curb the pandemic, it will be important to consider the balance between privacy and the public good.

- The roll-out of AI to combat coronavirus illustrates that new technologies' potential use is contingent upon the rules countries set for their design, development, deployment and use. Governments need to be capable of articulating parameters and principles to ensure that the design, development, deployment, and use of new technologies contribute to public health objectives while balancing societal and legal concerns.

- The Digital Inclusion Lab at Global Affairs Canada leverages innovative tools and partnerships to analyze the international human rights, freedoms, and inclusion implications of digital technology and online spaces. The lab is also looking at AI and recently released a report on COVID-19 and digital contact tracing, which contends that Canada should advocate a rights-based approach to the roll-out of contract tracing apps worldwide with a view to promoting human rights, democracy, and inclusion.

- In light of these considerations, policy makers must focus on using AI and corresponding apps responsibly; be wary of disproportionate impacts and singling out specific communities; validate systems and ensure sanitized, safe data is being used; and ensure these systems are transparent, explainable, robust, secure and safe.

CONCLUSION

- As the CAF may be called upon to respond to national emergencies, such as a second wave of COVID-19 or a future health emergency or natural disaster, the option to make use of AI enabled technology will increasingly become a reality. In making decisions about the use of such technology, DND/CAF should take the necessary time to weigh the potential benefits against the potential security and reputational risks.

Prepared by: Laurel Myers, Policy Officer, D DT Pol, 543-7178
Consulted by: Julia Dick, Policy Analyst, ADM DIA, 992-7946
Responsible Director: Kim Rebenchuk, D DT Pol, 995-7384
Responsible Director General: Jonathan Quinn, DG Contl Def Pol, 943-0886
Responsible Group Principal: Peter Hammerschmidt, ADM (Pol)
Date Prepared: 24 September, 2020